

Pending Claims, Amended Claims Under 37 C.F.R. § 1.116(b):

Claims 1-20, now pending, are submitted below which presents a clean version of the entire set of pending claims. Claims 3, 7, 12-19 were previously amended are presented in this response under 37 C.F.R. § 1.116(b) in form for consideration on appeal.

1. (Unchanged) A method for inspecting an encrypted data stream being transferred over a network between two endpoints, the data stream being encrypted using a session key known to both endpoints, the method comprising:

securely transferring the session key from one of the endpoints to an intermediary having access to the encrypted data stream;

decrypting the encrypted data stream at the intermediary using the session key; and

inspecting the data stream following decryption.

2. (Unchanged) A method as recited in claim 1, wherein securely transferring comprises:

encrypting the session key using a public key associated with the intermediary; and

sending the encrypted session key to the intermediary.

3. (Amended Once) A method as recited in claim 1, wherein securely transferring comprises:

encrypting the session key using a public key associated with the intermediary;

1 signing the encrypted session key using a private key associated with the
2 one of the endpoints; and

3 sending the signed and encrypted session key to the intermediary.

4
5 4. (Unchanged) A method as recited in claim 1, further comprising
6 storing the data stream at the intermediary.

7
8 5. (Unchanged) A method for inspecting an encrypted data stream being
9 transferred over a network between two endpoints and via an intermediary, the
10 data stream being encrypted using a session key known to both endpoints, the
11 method comprising:

12 storing a public key from a public/private key pair associated with one of
13 the endpoints at a key storage;

14 storing a public key from a public/private key pair associated with the
15 intermediary at the key storage;

16 obtaining, at said one endpoint, the intermediary's public key from the key
17 storage;

18 encrypting, at said one endpoint, the session key using the intermediary's
19 public key to produce an encrypted session key;

20 encrypting, at said one endpoint, the encrypted session key using a private
21 key from the public private key pair associated with said one endpoint to produce a
22 signed encrypted session key;

23 passing the signed encrypted session key to the intermediary;

24 obtaining, at the intermediary, the one endpoint's public key from the key
25 storage;

1 decrypting, at the intermediary, the signed encrypted session key using the
2 one endpoint's public key to return the encrypted session key;

3 decrypting, at the intermediary, the encrypted session key using the
4 intermediary's private key to return the session key; and

5 using the session key at the intermediary to decrypt the encrypted data
6 stream.

7
8 6. (Unchanged) In a network system in which an encrypted data stream
9 is transferred over a network between two endpoints and via an intermediary, the
10 data stream being encrypted using a session key known to both endpoints,
11 computer-readable media at one of the endpoints and at the intermediary storing
12 computer-executable instructions for performing the method as recited in claim 5.

13
14 7. (Amended Once) In a network system having an internal client that
15 exchanges encrypted data with an external client over a network and through a
16 firewall intermediate of the internal and external clients, the encrypted data being
17 encrypted using a session key known to the internal and external clients, a method
18 executed at the firewall comprising:

19 receiving an encrypted and signed session key from the internal client, the
20 encrypted and signed session key bearing a digital signature of the internal client;

21 authenticating the digital signature as belonging to the internal client;

22 decrypting the session key, and

23 decrypting the encrypted data being exchanged between the internal and
24 external clients using the session key.

25

1 8. (Unchanged) A method as recited in claim 7, wherein the encrypted
2 and signed session key is encrypted using a public key from a public/private key
3 pair associated with the firewall, and the decrypting comprises decrypting the
4 session key using a private key from the public/private key pair.

5
6 9. (Unchanged) A method as recited in claim 7, further comprising
7 inspecting the data in an unencrypted form.

8
9 10. (Unchanged) A method as recited in claim 7, further comprising
10 storing the data in an unencrypted form.

11
12 11. (Unchanged) In a network system having an external client that
13 exchanges encrypted data with an external client over a network and through a
14 firewall intermediate of the internal and external clients, the encrypted data being
15 encrypted using a session key known to the internal and external clients, a
16 computer-readable medium resident at the firewall storing computer-executable
17 instructions for performing method as recited in claim 7.

18
19 12. (Amended Once) A network system comprising:
20 an internal client device and an external client device configured to
21 communicate encrypted data over a network using virtual private network
22 communication, the data being encrypted using a session key;
23 an intermediary device having access to the encrypted data being
24 communicated between the internal client device and the external client device;

25

1 the internal client device being configured to securely transfer the session
2 key to the intermediary device; and

3 the intermediary device being configured to decrypt the data using the
4 session key and to inspect the data.

5
6 13. (Amended Once) A network system as recited in claim 12, wherein
7 the internal client device encrypts the session key prior to sending it to the
8 intermediary device.

9
10 14. (Amended Once) A network system as recited in claim 12, wherein
11 the internal client device encrypts and signs the session key prior to sending it to
12 the intermediary device.

13
14 15. (Amended Once) A network system as recited in claim 12, wherein
15 the intermediary device stores the data in unencrypted form.

16
17 16. (Amended Once) A software architecture for a network system
18 having two endpoints that exchange encrypted data over a network and through an
19 intermediary, the encrypted data being encrypted using a session key known to the
20 endpoints, comprising:

21 endpoint-resident code stored on computer readable media and executable
22 on a processor to encrypt the session key using a public key from a public/private
23 key pair associated with the intermediary and to sign the encrypted session key
24 with a digital signature, the endpoint-resident code being capable of sending the
25 signed and encrypted session key to the intermediary; and

1 intermediary-resident code stored on computer readable media and
2 executable on the processor to authenticate the digital signature and decrypt the
3 encrypted session key using a private key from the public/private key pair
4 associated with the intermediary, the intermediary-resident code using the session
5 key to decrypt the encrypted data as it is being exchanged between the two
6 endpoints.

7
8 17. (Amended Once) A software architecture as recited in claim 16,
9 wherein the intermediary-resident code inspects the data in unencrypted form.

10
11 18. (Amended Once) A software architecture as recited in claim 16,
12 wherein the intermediary-resident code stores the data in unencrypted form.

13
14 19. (Amended Once) In a network system having an internal client that
15 exchanges encrypted data with an external client over a network and through a
16 firewall intermediate of the internal and external clients, the encrypted data being
17 encrypted using a session key known to the internal and external clients, computer-
18 readable media distributed at the internal client and the firewall storing computer-
19 executable instructions for:

20 encrypting the session key at the internal client;
21 signing the encrypted session key with a digital signature associated with
22 the internal client;
23 passing the signed and encrypted session key to the intermediary;
24 authenticating, at the intermediary, the digital signature of the internal
25 client;